(12) PATENT **(11)** Application No. **AU 199933933 B2**
(19) AUSTRALIAN PATENT OFFICE **(10)** Patent No. **743933**

(54) Title
An entry system

(51)[7] International Patent Classification(s)
B60R 025/00 **H04L 009/32**
G08B 001/00

(21) Application No: **199933933** (22) Application Date: **1999.06.08**

(30) Priority Data

(31) Number	(32) Date	(33) Country
PP4752	**1998.07.20**	**AU**

(43) Publication Date : **2000.02.10**
(43) Publication Journal Date : **2000.02.10**
(44) Accepted Journal Date : **2002.02.07**

(71) Applicant(s)
Robert Bosch GmbH

(72) Inventor(s)
Peter Crowhurst; Frank Pavatich

(74) Agent/Attorney
DAVIES COLLISON CAVE,1 Little Collins Street,MELBOURNE VIC 3000

(56) Related Art
WO 93/25987
DE 4234822
US 4209783

ABSTRACT:

An entry system (2) including an electronic key (4) having a transmitter (6) and a secure area having a receiver (10), the transmitter (6) and receiver (10) being adapted to communicate to transmit authentication data, characterised in that the transmitter (6) transmits a signal, the receiver (10) converts the transmitted signal to spectral data, and the entry system (2) allows access to the secure area on transmission of the authentication data when the spectral data corresponds to a spectral signature of the transmitter (6).

Regulation 3.2

AUSTRALIA

Patents Act 1990

COMPLETE SPECIFICATION

FOR A STANDARD PATENT

(ORIGINAL)

Name of Applicant: **ROBERT BOSCH GmbH** of Postfach 30 02 20, D-70442 Stuttgart, Germany

Actual Inventor(s):

Address for Service: **DAVIES COLLISON CAVE**, Patent Attorneys, of 1 Little Collins Street, Melbourne, Victoria 3000, Australia

Invention Title: **"AN ENTRY SYSTEM"**

Details of Associated Provisional Application No: PP4752/98

The following statement is a full description of this invention, including the best method of performing it known to us:

AN ENTRY SYSTEM

The present invention relates to an entry system, and in particular to a passive entry system for vehicles.

Current passive entry systems for vehicles use a remote electronic key which incorporates a transmitter that transmits authentication data to a receiver located in the vehicle, when the key is within a predetermined range from the receiver. The communications protocol executed between the transmitter and the receiver uses a radio frequency interface to carry the transmitted data. The radio frequency (rf) interface has a limited range, to ensure the communication link is broken when a holder of the key moves away from the immediate vicinity of the vehicle.

Passive entry systems are susceptible to attack by unauthorised persons using a repeater system, placed between the vehicle and the key, which exploits rf amplifiers to establish the communication link when the key is not within the immediate vicinity of the vehicle. It is desired to provide a system which obviates this problem or at least provides a useful alternative.

In accordance with the present invention there is provided an entry system including an electronic key having a transmitter and a secure area having a receiver, said transmitter and receiver being adapted to communicate to transmit authentication data, characterised in that said transmitter transmits a signal, said receiver converts the transmitted signal to spectral data, and said entry system allows access to said secure area on transmission of said authentication data when said spectral data corresponds to a spectral signature of said transmitter.

Advantageously, the receiver may detect the presence of a repeater system when the spectral data represents application of a transfer characteristic of the repeater system.

The present invention also provides a method of allowing entry to a secure area, including:

receiving a transmitted signal;

converting the transmitted signal to spectral data;

comparing the spectral data with a spectral signature of a transmitter; and

allowing access to said secure area on receiving authentication data when said spectral data corresponds to said spectral signature.

A preferred embodiment of the present invention is hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a schematic diagram of a preferred embodiment of an entry system, with an intervening repeater station, and showing the signals transmitted and received;

Figure 2 is a schematic graph of received signal strength against frequency; and

Figure 3 is a block diagram of the entry system.

A passive entry system 2, as shown in the Figures, includes an electronic key 4 with a transmitter 6 and an induction coil antenna 7, a base station 8 with a receiver 10 and an induction coil antenna 12. The base station 8 is located in a secure area, such as a vehicle, and controls access to the secure area. When the key 4 is brought within a predetermined range from the antenna 12 of the receiver 10, the receiver 10 excites the key 4, so as to cause the transmitter 6 to begin transmission to the receiver 10. Data is transmitted using rf signals which establish a communications link between the key 4 and the base station 8. The data transmitted between the key 4 and the base station 8 is determined by a communications protocol which the key 4 and base station 8 adhere to, and which involves the transmission of authentication data from the key 4 to the receiver 10. Access to the secure area is only allowed by the base station 8 if the transmitted authentication data corresponds with authentication data stored by the base station 8.

To establish a communication link between the key 4 and the base station 8, when the key 4 is outside of the predetermined range from the receiver's antenna 12, a radio frequency repeater 16 can be inserted between the key 4 and the base station 8. To establish the communication link, the repeater 16 uses amplifiers which need to apply considerable gain to the signals transmitted by the system 2 in order to breach the distance between the key 4 and the base station 8. The amplifiers of any high gain repeater 16 have a transfer characteristic which, although ideally linear, is never linear in practice and will taper off to

a maximum gain. The repeater 16 will therefore perturb the signal transmitted by the key 4, and the linearity of the repeater 16 determines the amount of signal perturbation. The linearity of an amplifier can be measured, using a measurement known as a two tone measurement to determine the third order intercept point of the amplifier. The third order intercept point is a theoretical point when third order tones, generated by a mixing of fundamental transmission tones, intercept or interfere with the fundamental tones, in the sense that the third order signals from the amplifier have the same amplitude as the first order or fundamental signals. The third order intercept point (IP3) of an rf amplifier is a characteristic which can be determined by measuring the received signal strength of the third order inter-modulation tones received by a receiver.

Passive entry systems normally transmit data using a single rf tone. In order to detect the presence of a repeater 16, based on the signal perturbation it introduces, the entry system 2 of the preferred embodiment transmits two fundamental frequency tones 20 and 22, as shown by the transmitter spectrum 25. The two rf tones 20 and 22 can be used to transmit data, yet the accuracy of the two tone measurement subsequently performed by the receiver 10, as described below, may be only $\pm 5\%$. The accuracy of the measurement is $\pm 1\%$ if the key 4 transmits the tones 20 and 22 with a constant amplitude, for the two tone measurement, and then subsequently transmits the authentication data using rf modulation with one or both of the tones being the carrier signal.

In response to transmission of the fundamental tones 20 and 22, the receiver 10 will receive the tones and two third order inter-modulation tones 24 and 26, as shown in the frequency or spectral response 27 for the receiver 10. The fundamental tones 20 and 22, as shown in Figure 2, reside in adjacent frequency channels C2 and C3, whereas the inter-modulation tones 24 and 26 produced by mixing the fundamental tones will have a reduced amplitude and reside in a lower frequency channel C1 and a higher frequency channel C4. A received signal strength indicator (RSSI) is generated by most FM radio receiver semiconductors, and can provide a measurement of the amount of energy received in each of the channels C1 to C4. The RSSI output produced by the receiver 10 is a voltage that is proportional to the in band energy of the received signal in each of the measured channels C1 to C4. The RSSI for each channel can therefore be used to determine any variation introduced in the third order modulation tones 24 and 26 by the introduction of a repeater 16, due to the

non-linearity of the amplifiers of the repeater 16. To detect this variation, the entry system 2 is initiated by first establishing a normal communication link between the key 4 and the base station 8 within the predetermined range, measuring the RSSI for each channel C1 to C4, and recording this as a spectral signature for the transmitter 6 of the key 4. All future transmissions can then be similarly measured to determine whether any repeater has been introduced into the system to vary the amount of third order inter-modulation energy received. The difference in the third order tones received can further be used to determine a characteristic third order intercept point to identify the intercepting repeater 16. Detection of a repeater 16 by the base station 10, will ensure the base station 10 denies access to the secure area, even if the authentication data is validly received.

The transmitter 6, as shown in Figure 3, includes circuitry to transmit two constant tone signals, once the key 4 is excited by the receiver 10. The circuitry can include two radio frequency oscillators 30 and 32 for the tones, respectively, the outputs of which are combined in a combiner 34 for transmission on the antenna 7 of the transmitter 6. Alternatively, the circuitry may include a complex quadrature modulator that enables the generation of two tones separated by a multiple of the channel spacing used in the receiver 10.

The receiver 10 includes a radio FM receiver 36 connected to the antenna 12, an analogue/digital converter 38, a microcontroller 40, and a frequency synthesised local oscillator 42. The microcontroller 40 is programmed to control the frequency synthesiser 42, and to process data received from the A/D converter 38. The frequency synthesiser is used to select frequency channels to be processed by the FM receiver 36, which as discussed previously, generates an RSSI output for each of the four channels C1 to C4. The RSSI output for each channel is passed to the A/D converter for conversion into a binary word for processing by the microcontroller 40. The microcontroller 40 treats the binary word as spectral data representative of the received energy in each of the channels C1 to C4, and in turn uses the spectral data for comparison with a previously stored spectral signature for the transmitter 6.

The system 2 is initiated by placing the key 4 within the predetermined range from the antenna 12 so as to excite the key 4 and cause a transmission of the two fundamental tones. The spectral data received by the microcontroller 40 is then stored as the spectral signature

of the transmitter 6 for future comparison for all subsequent communications between the key 4 and the receiver 10.

The key 4 and the base station 8 accordingly execute the following steps when a communication link is subsequently established:

(i) Prior to the transmission of any authentication data, the two fundamental tones in channels C2 and C3 are simultaneously transmitted.

(ii) The frequency synthesiser 42 selects the four channels C1 to C4 and the FM receiver 36 produces an RSSI output for each of the channels.

(iii) The microcontroller 40 receives and processes the spectral data representative of the received signal levels for each of the channels, and this is compared with the stored spectral signature.

(iv) If there is any deviation between the spectral signature and the spectral data by more than $\pm 1\%$, the microcontroller 40 causes the base station 10 to halt the authentication procedure and prevent access to the secure area.

(v) The level of deviation between received spectral data and the spectral signature is recorded for subsequent analysis to determine a characteristic third order interception point to identify the attacking repeater 16. The number of attacks by the repeater 16 can also be stored.

(vi) When the base station 10 subsequently detects an authorised user and allows authorised access, the microcontroller 40 causes generation of a warning signal to indicate an attack has been made. The warning signal may be in a form of a displayed message, a warning lamp or an audio signal generated in the secure area, i.e. the vehicle.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawings.

The reference numerals in the following claims are not to be construed as imposing any limitations on the claims.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. An entry system including an electronic key having a transmitter and a secure area having a receiver, said transmitter and receiver being adapted to communicate to transmit authentication data, characterised in that said transmitter transmits a signal, said receiver converts the transmitted signal to spectral data, and said entry system allows access to said secure area on transmission of said authentication data when said spectral data corresponds to a spectral signature of said transmitter.

2. An entry system as claimed in claim 1, wherein said system is initiated by said transmitter transmitting said signal to said receiver, and said receiver converts the transmitted signal to said spectral data and stores said spectral data as said spectral signature.

3. An entry system as claimed in claim 1 or 2, wherein said signal comprises a spread spectrum.

4. An entry system as claimed in claim 1 or 2, wherein said signal comprises at least two tones, and said spectral data represents third order tones of said transmitted signal.

5. An entry system as claimed in claim 4, wherein said tones are constant in amplitude.

6. An entry system as claimed in claim 5, wherein said spectral data is generated based on the received signal strength of said transmitted signal in at least two frequency bands.

7. An entry system as claimed in claim 6, where said two frequency bands correspond to the frequencies of the third order tones, respectively.

8. An entry system as claimed in claim 7, wherein said receiver determines a difference between said spectral data and said spectral signature for use in identifying an unauthorised system.

9. An entry system as claimed in claim 7, wherein said authentication data is transmitted after transmitting said constant amplitude tones.

10. An entry system as claimed in claim 7, wherein said receiver, includes:

means for demodulating the transmitted signal for selected frequency bands and generating received signal strength signals for said bands; and

means for converting said received signal strength signals into said spectral data and comparing said spectral data with said spectral signature.

11. An entry system as claimed in claim 10, wherein said demodulating means includes a frequency synthesiser for selecting said bands, and said converter means includes a microcontroller for controlling said frequency synthesiser.

12. An entry system as claimed in any one of the preceding claims, wherein said secure area is within a vehicle.

13. A vehicle including an entry system as claimed in any one of the preceding claims.

14. A method of allowing entry to a secure area, including:

receiving a transmitted signal;

converting the transmitted signal to spectral data;

comparing the spectral data with a spectral signature of a transmitter; and

allowing access to said secure area on receiving authentication data when said spectral data corresponds to said spectral signature.

15. A method as claimed in claim 14, including transmitting at least two tones, and wherein said spectral data represents third order tones of the transmitted signal.

16. An entry system substantially as hereinbefore described with reference to the accompanying drawings.

17. A method of allowing entry to a secure area substantially as hereinbefore described with reference to the accompanying drawings.

DATED this 22nd day of November 2001

Robert Bosch GmbH

By its Patent Attorneys

DAVIES COLLISON CAVE

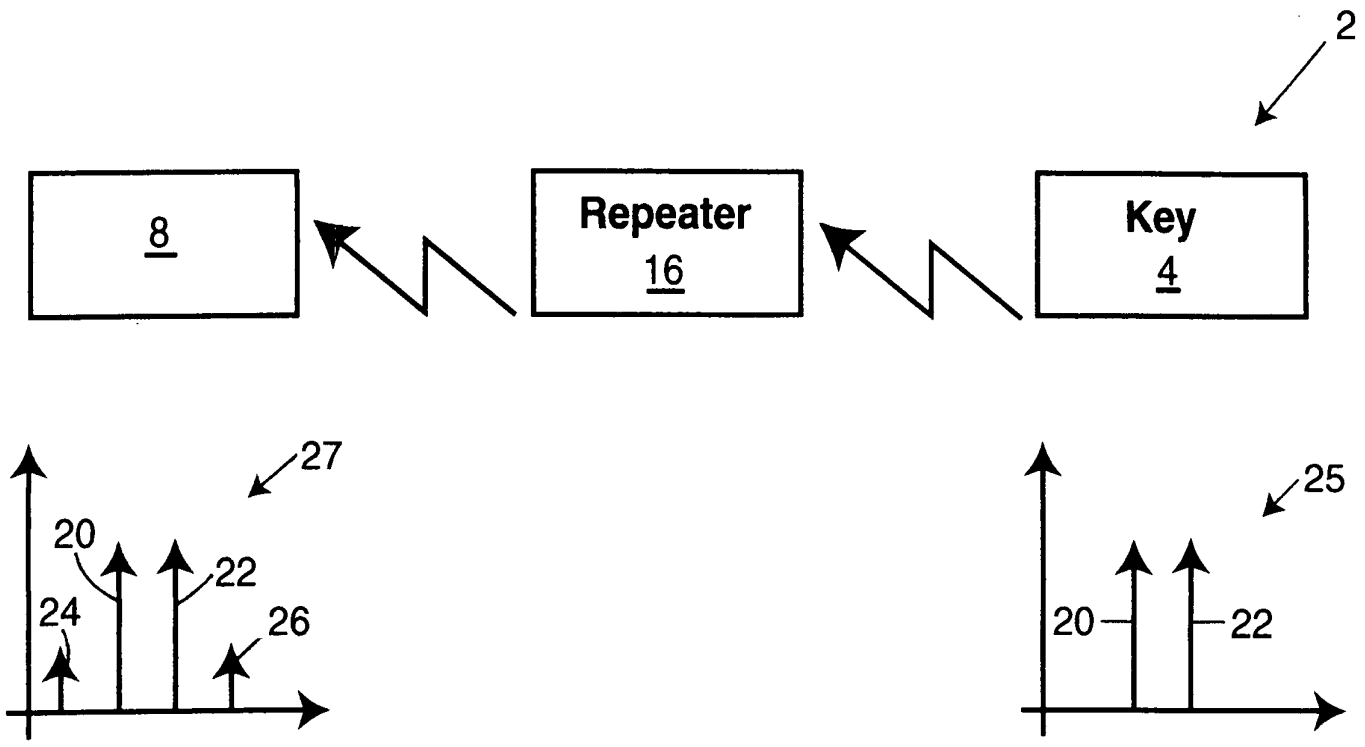

FIG 1

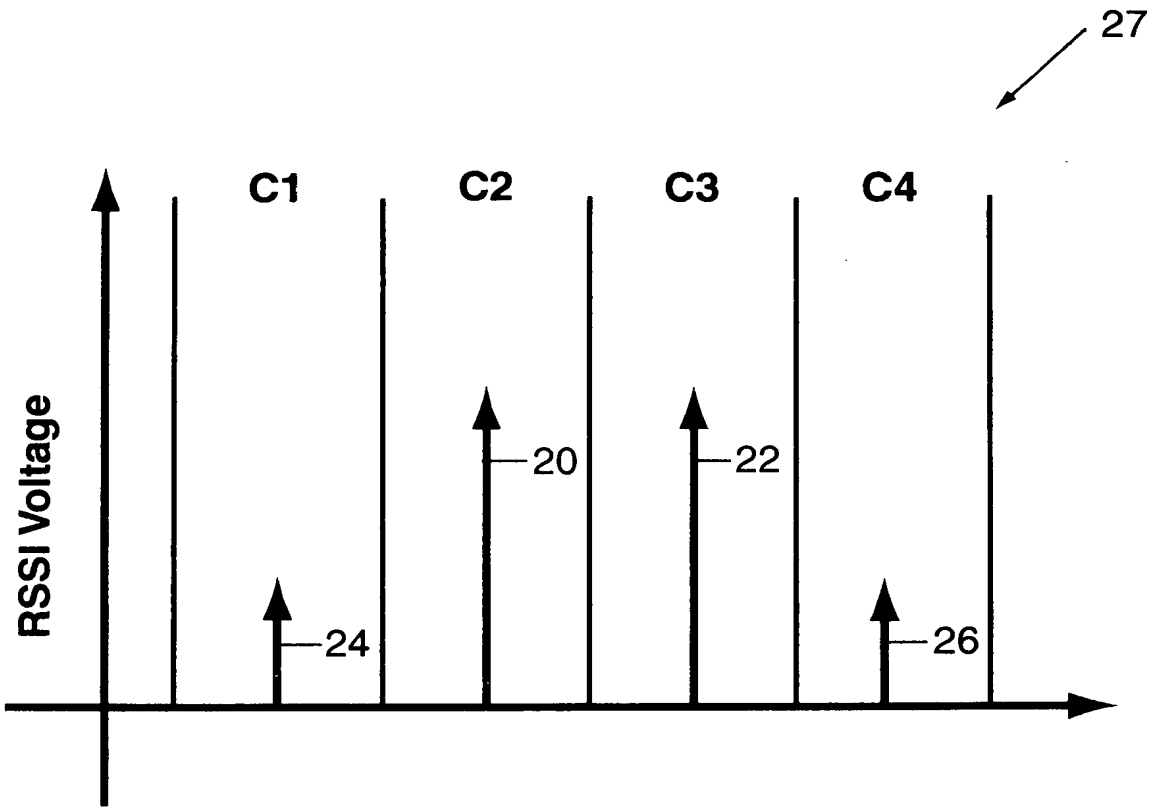

FIG 2

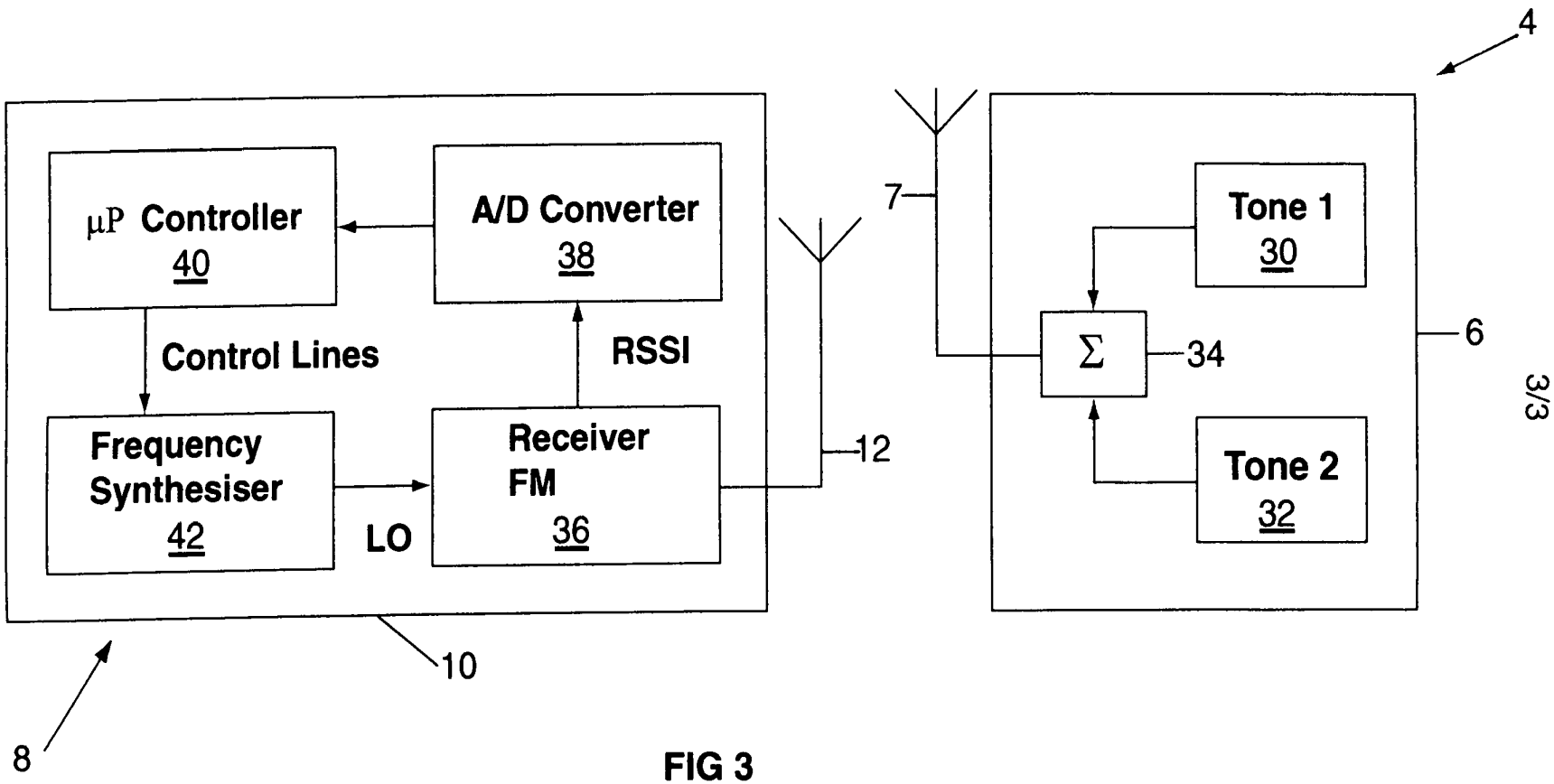
4
μP Controller
40
A/D Converter
38
Control Lines
RSSI
Frequency
Synthesiser
42
LO
Receiver
FM
36
12
10
8
7
Tone 1
30
Σ
34
6
Tone 2
32

FIG 3